

# PROCESS OF "PRIMOVERIZATION" OF NUMBERS OF THE FORM $a^n - 1$

VLADIMIR SHEVELEV

**ABSTRACT.** We call an integer  $N > 1$  primover to base  $a$  if it either prime or overpseudoprime to base  $a$ . We prove, in particular, that every Fermat number is primover to base 2. We also indicate a simple process of receiving of primover divisors of numbers of the form  $a^n - 1$ .

## 1. INTRODUCTION

Let  $a > 1$  be an integer. For an odd  $n > 1$ , consider the number  $r = r_a(n)$  of distinct cyclotomic cosets of  $a > 1$  modulo  $n$  [1, pp.104-105]. Note that, if  $C_1, \dots, C_r$  are all different cyclotomic cosets of  $a \pmod n$ , then

$$(1) \quad \bigcup_{j=1}^r C_j = \{1, 2, \dots, n-1\}, \quad C_{j_1} \cap C_{j_2} = \emptyset, \quad j_1 \neq j_2.$$

For the least common multiple of  $|C_1|, \dots, |C_r|$  we have

$$(2) \quad [|C_1|, \dots, |C_r|] = h,$$

where  $h = h_a(n)$  is the multiplicative order of  $a$  modulo  $n$ . (This follows easily, e.g., from Exercise 3, p. 104 in [2]).

It is easy to see that for odd prime  $p$  we have

$$(3) \quad |C_1| = \dots = |C_r|$$

such that

$$(4) \quad p = rh + 1.$$

**Definition 1.** We call odd composite number  $n$  overpseudoprime to base  $a$  ( $n \in \mathbb{S}_a$ ) if

$$(5) \quad n = r_a(n)h_a(n) + 1.$$

Let  $n$  be odd composite number with the prime factorization

$$(6) \quad n = p_1^{l_1} \cdots p_k^{l_k}.$$

In [3] we proved the following criterion.

**Theorem 1.** *The composite number  $n$  (6) is overpseudoprime to base  $a$  if and only if for all nonzero vectors  $(i_1, \dots, i_k) \leq (l_1, \dots, l_k)$  we have*

$$(7) \quad h_a(n) = h_a(p_1^{i_1} \cdots p_k^{i_k}).$$

**Corollary 1.** *Every two overpseudoprimes  $n_1$  and  $n_2$  for which  $h_a(n_1) \neq h_a(n_2)$  are coprimes.*

Notice that, every overpseudoprime to base  $a$  is always superpseudoprime and strong pseudoprime to the same base ( see Theorems 12-13 in [3]). Besides, in [3] we proved, in particular, the following result.

**Theorem 2.** *If  $p$  is prime then  $2^p - 1$  is either prime or overpseudoprime to base 2.*

Note that, prime divisors of overpseudoprime  $n$  are primitive divisors of  $2^{h(n)} - 1$ . Thus, all overpseudoprimes to base 2 are generated by the set of primitive divisors of the sequence  $(2^n - 1)_{n \geq 1}$ .

Denote by  $Ov_2(x)$  the number of overpseudoprimes to base 2 not exceeding  $x$ . In the next paper of our cycle we shall prove that

$$(8) \quad Ov_2(x) = o(x^\varepsilon),$$

where  $\varepsilon > 0$  is arbitrary small for sufficiently large  $x$ .

**Definition 2.** *An integer which is either prime or overpseudoprime to base  $a$  we call primover to the same base.*

The following theorem complements Theorem 2.

**Theorem 3.** *If  $n$  is primover to base 2, then  $2^n - 1$  is primover to base 2 if and only if  $n$  is prime.*

**Proof.** If  $n$  is prime then, by Theorem 2,  $2^n - 1$  is primover to base 2. Let  $n$  be not prime. If it contains two different prime divisors  $p < q$ , then  $h_2(2^p - 1) = p < q = h_2(2^q - 1)$ . This means that  $2^n - 1$ , which is multiple of  $2^p - 1$  and of  $2^q - 1$ , is neither prime, nor overpseudoprime to base 2. At last, if  $n = p^k$  then  $h_2(2^p - 1) = p < h_2(2^{p^2} - 1)$  and again  $n$  is not primover

to base 2. ■

In this paper we indicate a very simple process of a constructive construction of (large) primovers to base  $a$  from numbers of the form  $a^n - 1$ .

## 2. PROCESS OF "PRIMOVERIZATION"

We start with the following result.

**Theorem 4.** *For  $n \geq 1$  every Fermat number  $F_n = 2^{2^{n-1}} + 1$  is primover to base 2.*

**Proof.** Let  $d > 1$  be a divisor of  $F_n$ . Then  $2^{2^{n-1}} \equiv -1 \pmod{d}$  and  $2^{2^n} \equiv 1 \pmod{d}$ . Thus,  $h_2(d) \leq 2^d$ . But  $h_2(d) | 2^n$ . Therefore,  $h_2(n) = 2^i, i \leq n$ . If  $i \leq n - 1$  then  $d$  divides  $2^{2^{i-1}}$  and does not divide  $2^{2^{i-1}-1}$ . Hence,  $d | 2^{2^{i-1}} + 1 = F_i$ . It is impossible since for  $i \leq n - 1$  we have  $(F_i, F_n) = 1$ . Therefore, for every divisor  $d > 1$  of  $F_n$  we have  $h_2(d) = 2^n$  and, by Theorem 1, if  $F_n$  is not prime, then it is overpseudoprime to base 2. ■ Thus, if the well known Hardy-Wright conjecture about the finiteness of the number of Fermat primes is true, then the expression  $2^{2^{n-1}} + 1$  gives since some  $n$  only overpseudoprimes to base 2. On the other hand, by Theorem 3, the expression  $2^{F_n} - 1$  gives since the corresponding  $n$  neither primes nor overpseudoprimes to base 2. It is interesting also to notice that, if  $Pr_2(x)$  denotes the number of primovers to base 2 not exceeding  $x$ , then by (8) we have  $Over_2(x) = \pi(x) + o(x^\epsilon)$ . In spite of this very small difference, the problem of finding of a useful formula which gives only primes is unsolved until now, while the simple and very useful in mathematics Fermat construction gives only primovers to base 2.

**Example 1.** *For  $n = 6$  we obtain the following primover to base 2: 4294967297. It is 2315-th strong pseudoprime to base 2 (see [4, Seq. A001262]).*

Quite analogously one can prove the following generalization of Theorem 4.

**Theorem 5.** *For  $n \geq 1$  and even  $a \geq 2$  every generalized Fermat number  $F_n^{(a)} = a^{2^{n-1}} + 1$  is primover to base  $a$ .*

The equality  $a^{2^{n-1}} + 1 = \frac{a^{2^n} - 1}{a^{2^{n-1}} - 1}$  prompts a way of "primoverization" of numbers of the form  $2^m - 1$  and, in more general, of the form  $a^m - 1$ .

**Theorem 6.** *If  $p < q$  are primes, then the number*

$$N = \frac{(a-1)(a^{pq}-1)}{(a^p-1)(a^q-1)}$$

*is primover to base  $a$  if and only if  $(N, (a^p-1)(a^q-1)) = 1$ .*

**Proof.** Notice, that  $(a^p-1, a^q-1) = a-1$  and, therefore,  $N$  is integer. Let  $(N, (a^p-1)(a^q-1)) = 1$  and  $d > 1$  be a divisor of  $N$ . Then  $d$  is a divisor of  $a^{pq}-1$  and, hence,  $h_a(d) | pq$ . But if  $h_a(d) = p$  then  $d | a^p-1$ . This contradicts to the condition. By the same arguments  $h_a(d) \neq q$ . Thus,  $h_a(d) = pq$  and does not depend on  $d$ . Therefore, using Theorem 1, we conclude that  $N$  is primover. Conversely, let  $N$  be primover. Then for every its divisor  $d > 1$  we have  $h_a(d) = pq$ . Therefore,  $d$  divide neither  $a^p-1$  nor  $a^q-1$ . Thus,  $(N, (a^p-1)(a^q-1)) = 1$ . ■

**Example 2.** *For  $a = 2, p = 5, q = 7$  we obtain a primover 8727391 which is the 150-th strong pseudoprime to base 2 (see [4, Seq. A001262]).*

Quite analogously one can prove the following result.

**Theorem 7.** *If  $p$  is prime, then*

$$N = \frac{a^{p^n} - 1}{a^{p^{n-1}} - 1}$$

*is primover to base  $a$  if and only if  $(N, a^{p^{n-1}} - 1) = 1$ .*

**Example 3.** *For  $a = 2, p = 5, n = 2$  we obtain a primover 1082401 which is the 50-th strong pseudoprime to base 2 (see [4, Seq. A001262]).*

Let  $n$  is a composite squarefree number and its prime factorization is  $n = p_1 \cdot \dots \cdot p_t$ . Let to each combination of  $k \geq 0$  elements  $i_1, \dots, i_k$  from set  $(1, \dots, t)$  corresponds the number

$$a^{p_{i_1} \cdots p_{i_k}} - 1 = m_n(i_1, \dots, i_k)$$

(in case of  $k = 0$  we put  $m_n = a - 1$ ).

The following result, which could be proved using induction, generalizes Theorem 6.

**Theorem 8.** *The number*

$$N = \frac{\prod_{k \geq 0, k \equiv t \pmod{2}, 1 \leq i_1 < \dots < i_k \leq t} m_n(i_1, \dots, i_k)}{\prod_{k \geq 0, k \equiv t-1 \pmod{2}, 1 \leq i_1 < \dots < i_k \leq t} m_n(i_1, \dots, i_k)}$$

*is primover to base  $a$  if and only if the number  $a^{p_1 \cdots p_t} - 1$  is coprime to  $\frac{a^{p_1 \cdots p_t} - 1}{N}$ .*

**Example 4.** For  $a = 2, t = 3, p_1 = 2, p_2 = 5, P_3 = 7$  we obtain a primover 24214051 which is the 254-th strong pseudopime to base 2 (see [4, Seq. A001262]).

Furthermore, using the construction of Theorem 7, we obtain the following generalization of Theorem 6.

**Theorem 9.** If  $p < q$  are primes then, for  $a \geq 1, b \geq 1$ , the number

$$N = \frac{(a^{p^a q^b} - 1)(a^{p^{a-1} q^{b-1}} - 1)}{(a^{p^{a-1} q^b} - 1)(a^{p^a q^{b-1}} - 1)}$$

is primover to base  $a$  if and only if the number  $a^{p^a q^b} - 1$  is coprime to

$$\frac{(a^{p^{a-1} q^b} - 1)(a^{p^a q^{b-1}} - 1)}{(a^{p^{a-1} q^{b-1}} - 1)}.$$

In order to write a generalization we need to represent a nonnegative integer  $m < 2^k$  in the  $k$ -digit binary expansion (probably, with some 0's before the first 1). It is known, that  $m$  is called odious (evil) if the number of 1's in its binary expansion is odd (even). In the general case of composite number  $n = p_1^{l_1} \cdots p_k^{l_k}$  it could be obtained the following result.

**Theorem 10.** The number

$$(9) \quad N = \frac{\prod (a^{p_1^{l_1 - i_1} \cdots p_k^{l_k - i_k}} - 1)}{\prod (a^{p_1^{l_1 - j_1} \cdots p_k^{l_k - j_k}} - 1)},$$

where  $(i_1, \dots, i_k)$  runs the vectors of binary digits of all  $k$ -digit evil numbers from  $[0, 2^k - 1]$ , while  $(j_1, \dots, j_k)$  runs the vectors of binary digits of all  $k$ -digit odious numbers from the same segment, is primover to base  $a$  if and only if  $a^{p_1^{l_1} \cdots p_k^{l_k}} - 1$  is coprime to  $\frac{a^{p_1^{l_1} \cdots p_k^{l_k}} - 1}{N}$ .

**Definition 3.** Let  $n = p_1^{l_1} \cdots p_k^{l_k}$ . We call the number  $N$ , which is defined by (9), the primitive primover cofactor of  $a^n - 1$ , writing  $N = \text{Pr}(a^n - 1)$ .

Using induction, we obtain the following result.

**Theorem 11.** If in the expression for primover cofactor  $N$  (9) to drop in all factors  $(-1)$ 's, then we obtain  $a^{\varphi(n)}$ , where  $\varphi(n)$  is the Euler function.

Finally, we find a lower estimate of the primitive primover cofactor of  $a^n - 1$ .

**Theorem 12.** There exist a positive constant  $C_1$  such that

$$\text{Pr}(a^n - 1) \geq (a^n - 1)^{C_1 / \ln \ln n}.$$

**Proof** easily follows from Theorem 11 and the well-known Landau inequality  $\varphi(n) \geq Cn/\ln \ln n$ . ■

#### REFERENCES

- [1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier/North Holland, 1977.
- [2] D. Redmond, *Number Theory: an Introduction*, Marcel Dekker, N.Y., 1996.
- [3] V. Shevelev, *Overpseudoprimes, Mersenne numbers and Wieferich primes*, <http://arxiv.org/abs/0806.3412>.
- [4] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences* (<http://www.research.att.com>).

DEPARTMENT OF MATHEMATICS, BEN-GURION UNIVERSITY OF THE NEGEV, BEER-SHEVA 84105, ISRAEL. E-MAIL: SHEVELEV@BGU.AC.IL